КИБЕРУГРОЗЫ 2023 ДЛЯ ПРОМЫШЛЕННОГО СЕКТОРА

Часть 1

ROOT LEVEL RESOURCES

Основные тренды

Количество атак на компании промышленного сектора в 2022 увеличилось на 19% (обнаружено 295 инцидента).

Группировка APT41, спонсируемая Китаем, продолжает атаковать технологический и производственный секторы. Группе приписывают кампанию CuckooBees, в рамках которой с 2019 года велась тайная слежка за предприятиями в Северной Америке, Европе и Азии.

Полной защиты от прогосударственных хакеров не дают даже изолированные сети air gap. К примеру, китайский инструмент Daxin успешно работал в этих сетях, оставаясь незамеченным более 10 лет.

Tropic Trooper (еще одна китайская группа) использовала троян xPack для атаки на производственную организацию Тайваня и оставалась в сети компании 175 дней.

Киберпреступные группы, атакующие промышленный сектор

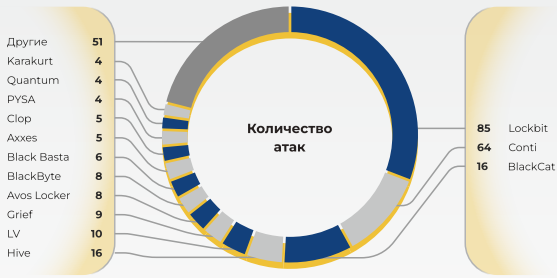
295

В 2022 было обнаружено **295 атак** групп шифровальщиков на промышленные компании.

Это на **19%** больше, чем в 2021

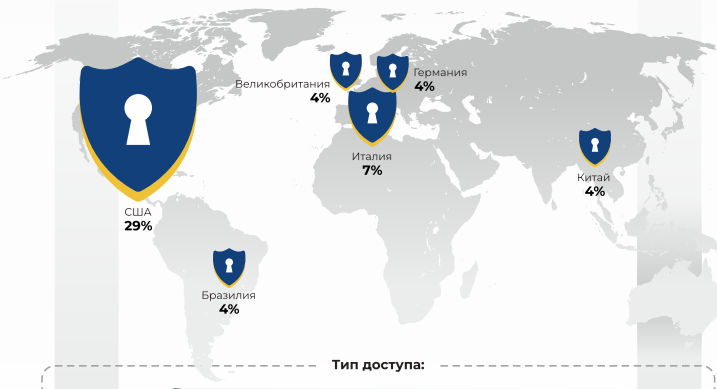
Больше всего доступов принадлежит компаниям США (31%), Германии (11%) и Италии (9%)

География атак выглядит следующим образом:

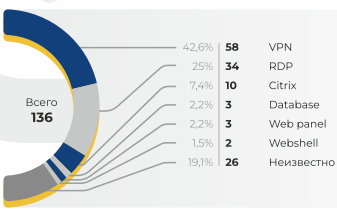


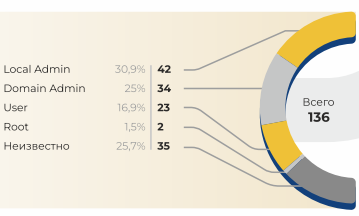
Проанализировав рынок брокеров доступов 2022 в данной индустрии, специалистами было обнаружено **136 доступа** к промышленным компаниям, выставленных на продажу киберпреступниками. Это на **33%** больше, чем в 2021.

Больше всего доступов принадлежит:



Тип доступа:





Брокеры, которые чаще всего продавали доступы к промышленным компаниям:

Novelli

15 RDP доступов, 9 из которых компании из Латинской Америки.

Практически все доступы с правами администратора – локального или доменного

orangecake

15 доступов, большая часть из которых VPN.

Более половины доступов приходится на Европу

Nei

7 VPN доступов за сентябрь и декабрь 2021 по всему миру.

5 из них с правами локального администратора

Наиболее активными группами в атаках на промышленные компании 2022 были Lockbit (29%), Conti (22%) и BlackCat (5%), Hive (5%):